## REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed March 23, 2005. In the Office Action, claims 1-8, 15-20, 22, 25 and 30-32 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting. In addition, claim 22 was objected due to a grammatical error. Moreover, claims 15-17 and 20-22 were rejected under 35 U.S.C. §102(e), claims 18-19 were rejected under 35 U.S.C. §112, and claims 1-14, 18-19, 23-26 and 30-32 were rejected under 35 U.S.C. §103(a).

Applicant respectfully traverses these rejections in their entirety and requests reconsideration of the allowability of claims 1-26 and 30-34. Claims 1-2, 4-7, 10-11, 14-18, 21-22, 24-26 and 30-31 have been revised. Claims 33 and 34 have been added.

### *Request for Examiner's Interview*

The Examiner is respectfully requested to contact the undersigned by telephone at the phone number listed below if after review, such claims are still not in condition for allowance. This telephone conference would greatly facilitate the examination of the present application. The undersigned attorney can be reached at the telephone number listed below.

### *Provisional Obviousness-type Double Patenting*

Claims 1-8, 15-20, 22, 25 and 30-32 were provisionally rejected under the judicially created doctrine of obviousness-type double based on a co-pending Continuation-In-Part (CIP) application (Application No. 09/904,962). Due to the "provisional" nature of this objection, Applicant respectfully offers to submit an executed terminal disclaimer to overcome the obviousness-type double patenting rejection provided the pending claims are in condition for allowance.

### *Objection of Claim 22*

Claim 22 was objected due to an alleged grammatical error. Applicant has revised claim 22 and respectfully requests the Examiner to withdraw the outstanding objection.

### *Rejection Under 35 U.S.C. §112, Second Paragraph*

Claims 18-19 were rejected under 35 U.S.C. §112 (second paragraph) as being allegedly indefinite. Applicant has revised claim 18 to correct an informality (antecedent basis) associated with claim 18. Based on this revision, Applicant respectfully requests the Examiner to withdraw the outstanding §112 rejection.

### *Rejection Under 35 U.S.C. § 102*

Claims 15-17 and 20-22 were rejected under 35 U.S.C. §102(e) as being anticipated by Barbir (U.S. Patent No. 6,122,379). Applicant respectfully requests the Examiner to withdraw the rejection because a *prima facie* case of anticipation has not been established.

As the Examiner is aware, to anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Vergegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the...claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989).

For instance, with respect to independent claim 15, Applicant respectfully submits that Barbir does not describe *encryption logic to perform a stream cipher operation* on input data *segmented in random sized blocks forming a sequence of blocks using an encryption key, the size of each block of the sequence of blocks varying in response to changes in the input data.* Emphasis added. These limitations are explicitly set forth in claim 15.

In contrast, Barbir teaches a modeling method that enables real time systems to perform simultaneous compression and encryption. This modeling method is used in conjunction with a coder and a random number generator to compress data in a secure fashion. *See column 6, lines 53-55 of Barbir*. Hence, the stream cipher as described in Barbir is used for secure data compression, and prior to the operations of the coder that performs the encryption operations. More specifically, Barbir teaches a modeling method that uses an encryption key or a seed with a random number generator, such as a stream cipher in conjunction with a modeler and a coder, to compress data. *See column 5, lines 27-30 of Barbir*. Barbir describes a [pseudo]random number generator (RNG) that is used to generate a sequence of blocks with different sizes. *See FIG. 4, step 40 of Barbir*. However, the sequence of blocks would be similarly sized for a given encryption key, which contradicts the claimed invention where the sizes of the blocks are not constant but vary as the input data changes.

Thus, in light of the foregoing, withdrawal of the §102(e) rejection as applied to independent claim 15 as well as claims 16-17 and 20-22 dependent thereon is respectfully requested. Applicant respectfully reserves the right to further submit additional grounds for traversing the rejection is an appeal is warranted.

## *Rejection Under 35 U.S.C. § 103*

A. §103 REJECTION OF CLAIMS 1-5, 14, 18-19 AND 30-32

Claims 1-5, 14, 18-19 and 30-32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Barbir in view of Zhang (U.S. Patent No. 6,154,541). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).* Herein, the combined teachings of the cited references fail to describe or suggest all the claim limitations.

With respect to independent claims 1 and 30, Applicant respectfully submits that neither Barbir nor Zhang, alone or in combination, teach or suggest the following:

> a first software routine to divide incoming plain text into variable-sized blocks at least three blocks being divided with three different sizes, a *size of each variable-sized block changing in response to variations of an internal state of the computing device caused by changes in the incoming plain text*; and
>
> a second software routine to *convert the plain text into cipher text based on an encryption key and an internal identifier.* Emphasis added.

First, the stream cipher of Barbir is involved with a modeling method that uses an encryption key or a seed with a random number generator, such as a stream cipher in conjunction with a modeler and a coder, to compress the data in a secure fashion. *See column 5, lines 27-30.* The modeling method induces randomness into the coding probabilities. This is accomplished through use of a stream cipher that divides the block into sub-blocks of variable size. However, it is evident that this technique is designed as an external input source to the coder, and is not used as the coder itself. The hybrid stream cipher is a coder that performs the encryption

operation as now claimed in claims 1 and 30 as well as the "*encrytion* logic" clarification of claim 15.

Hence, based on the teachings of Barbir and Zhang, a *prima facie* case of obviousness has not been established because the combined teachings of Barbir nor Zhang fail to describe or suggest all the claim limitations. As an example, the stream cipher operations of Barbir are directed to a modeling scheme and are not involved with cryptographic functionality such as encryption.

Second, neither Barbir nor Zhang suggests any operation before by software where the incoming plain text is divided into variable-sized blocks with a size of each variable-sized block changing in response to in response to variations of an internal state of the computing device caused by changes in the incoming plain text. Zhang is devoid of any teaching of block segmentation as claimed. Barbir, however, apparently teaches a RNG that is used to generate a sequence of blocks with different sizes, where the sequence of size of blocks would be the same for a given encryption key. Hence, the sizes of the blocks would be constant for the same encryption key and would not vary as the incoming plain text changes.

Thirdly, the techniques of re-seeding or key generation as taught by Zhang are directed only at the input or output, but not within the encryption process as claimed. Hence, the teachings of Zhang provide no suggestion or motivation to particular operations supported by software of a hybrid stream cipher as claimed. In fact, for the hybrid stream cipher, the non-linear function as set forth in dependent claims 2, 18 and 31 operates as an integral routine of the hybrid stream cipher (encryption) process as claimed.

Therefore, Applicant respectfully submits that neither Barbir nor Zhang, alone or in combination, disclose or suggest each and every limitation set forth in independent claims 1 and 30 as well as dependent claims 2-5, 14, 18-19 and 31-32. Applicant respectfully reserves the right to further submit additional grounds for traversing the rejection is an appeal is warranted. Withdrawal of the outstanding §103(a) rejection is respectfully requested.

B. §103 REJECTION OF CLAIMS 6-9 AND 25

Claims 6-9 and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Barbir in view of Zhang and Moskowitz (U.S. Patent No. 5,822,432). Applicant respectfully traverses the rejection in its entirety because a *prima facie* case of obviousness has not been established because neither Barbir, Zhang nor Moskowitz, alone or in any combination, suggests a third software routine to automatically determine if a plurality of random data elements are to be distributed within the cipher text without user intervention.

More specifically, with respect to claims 6-9, the Office Action states that Barbir does not provide any teaching of the third software routine as claimed, but it is alleged that Moskowitz provides such teachings through a human interactive digital watermarking process. As printed on column 5, lines 51-62 of Moskowitz, "[u]sing a mouse and/or a keyboard, the engineer can scroll through the signal slowly marking out time segments or frequency band minima and maxima which dictate where, at what frequencies, and at what encoding signal level a watermark signal is to be encoded into the content, given a random or pseudo random key sequence." Hence, this technique requires an engineer to identify where the content is to be inserted, which contradicts the claimed hybrid stream cipher where random data elements are *automatically* added to the *cipher text* without user intervention (claim 6) and the chosen degree of randomness is based on the internal state of the computing device (see claim 33).

With respect to claim 25, it is noted that the cipher text varies with the content of the plain text, where the techniques of Barbir, Zhang, and Moskowitz do not describe or suggest such variations.

Therefore, Applicant respectfully request that the outstanding §103(a) rejection as applied to claims 6-9 and 25 be withdrawn. Applicant respectfully reserves the right to further submit additional grounds for traversing the rejection is an appeal is warranted.

C. §103 Rejection of Claims 10-13 and 26

Claims 10-13 and 26 were rejected under 35 U.S.C. §103(a) as being unpatentable over Barbir in view of Zhang and Schneier (Applied Cryptography). Applicant respectfully traverses the rejection in its entirety because a *prima facie* case of obviousness has not been established for these claims. Herein, Schneier states that "whitening is the name given to the technique of XORing some key material with the *input to a block algorithm*, and XORing some other key material with the output." *See Page 366 of Schneier.* However, Schneier teaches the process of whitening or obfuscating at the input before the data is applied to the encryption process, which differs from the claimed invention where obfuscation occurs *within* the encryption process **which depends on the varying internal state of the computer device, which is equivalent to the internal state of the cipher**. *Emphasis added.* **Obfuscation as taught by Schneier does not vary the length of the cipher text, whereas the process of mixing changes the length of the cipher text (and thus output stream of claim 11) dynamically based on the internal state of the computing device, which varies with variations in the incoming plain text (input data) as set forth in claim 25 upon which claim 26 depends.** Hence, the process used by the hybrid cipher as claimed differs from the teachings of Schneier.

In addition, based on the dependency of claims 10-13 and 26 on independent claims 1 and 25, believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traverse is warranted. Applicant reserves the right to present such arguments in an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claims 10-13 and 26 is respectfully requested.

D. §103 Rejection of Claims 23-24

Claims 23-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Barbir in view of Schneier (Applied Cryptography). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for these claims. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for these claims. However, based on the dependency of claims 23-24 on independent claim 15, believed by Applicant to be in condition for allowance, no further discussion as to the

grounds for traverse is warranted. Applicant reserves the right to present such arguments in an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claims 23-24 is respectfully requested.

***Conclusion***

In view of the remarks made above, it is respectfully submitted that pending claims 1-26 and 30-34 define the subject invention over the prior art of record. Thus, Applicant respectfully submits that all the pending claims are in condition for allowance, and such action is earnestly solicited at the earliest possible date.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 06/23/2005 By _____

William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

---

***CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)***

*I hereby certify that this correspondence is, on the date shown below, being:*

**MAILING**

☒ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: 06/23/2005

**FACSIMILE**

☐ *transmitted by facsimile to the Patent and Trademark Office.*

*Susan McFarlane* 06/23/2005
*Susan McFarlane* *Date*